Белорусский государственный университет

УТВЕРЖДАЮ
Декан гуманитарного факультета
_____ В.Е.Гурский
(подпись) (И.О.Фамилия)
05.12.2012
(дата утверждения)
Регистрационный № УД-2012-1328/р.

Теория информации
(название дисциплины)

Учебная программа для специальности:
1-31 03 07 Прикладная информатика
(код специальности) (наименование специальности)

Факультет гуманитарный
(название факультета)

Кафедра информационных технологий
(название кафедры)

Курс 3
Семестр 6
Лекции 20
(количество часов)

Экзамен
(семестр)

Практические (семинарские) занятия
(количество часов)

Зачет 6
(семестр)

Лабораторные Занятия 14
(количество часов)

Курсовой проект (работа) _____
(семестр)

КСР
(количество часов)

Всего аудиторных часов по дисциплине
68
(количество часов)

Всего часов по дисциплине 34
(количество часов)

Форма получения высшего образования *очная*

Составил Седенков Владимир Михайлович, ст. преподаватель
(И.О.Фамилия, степень, звание)

2012 г.

Учебная программа составлена на основе типовой программы по курсу «Теория информации» №TD-P.216/тип от 16.06.2010 г.

Рассмотрена и рекомендована к утверждению на заседании кафедры информационных технологий

Пр №7 от 11.04.2012г.
(дата, номер протокола)

Заведующий кафедрой
_____ С.В.Царик
(подпись)

Одобрена и рекомендована к утверждению учебно-методической (методической) комиссией гуманитарного факультета/общеуниверситетской кафедры

Пр №5 от 21.05.2012г.
(дата, номер протокола)

Председатель
_____ О.В. Немкович
(подпись) *(И.О.Фамилия)*

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная программа по дисциплине «Теория информации и кодирование» для студентов III курса специальности «Современные иностранные языки» в объеме 68 учеб.часов (28—лекционные,28—практические, 12—лабараторные) разработана на основе типовой программы, регистрационный номер № ТД-86/тип, 2006г.

ЦЕЛЕВАЯ УСТАНОВКА

Изучение дисциплины «Теория информации и кодирование " имеет целью:

- ознакомить студентов с основными положениями теории информации и кодированием, являющимися необходимым компонентом математического образования и освоение которых обеспечит осознанное понимание многих разделов специальных дисциплин.
- сформировать умения грамотно анализировать основные проблемы, возникающие в практической деятельности специалиста гуманитарного профиля;
- научить будущих специалистов гуманитарного профиля применять полученные знания по теории информации и кодирование в практической деятельности;
- привить умение самостоятельно, посредством математического аппарата, осваивать реальные, характерные для специальности задачи;
- развить логическое мышление, аналитические способности, интеллект, необходимые для решения научных и практических задач гуманитарного профиля.

ЗАДАЧИ ДИСЦИПЛИНЫ:

- обеспечить овладение студентами теоретических основ данного курса, добиться четкого знания определений и основных теорем изучаемых разделов курса.
- выработать четкое овладение основными методами решения задач;
- выработать умение формулировать задачи гуманитарного профиля в точных и строгих соотношениях с использованием соответствующих математических символов;
- выработать понимание универсальности математических методов в задачах описания явлений и процессов в разных областях практической деятельности;
- формирование у студентов научного мировоззрения, рассмотрения предметов и явлений во всей их определенности, без искажений;
- подготовка высококвалифицированного специалиста, развитие его интеллекта и способностей к логическому и алгоритмическому мышлению.

Цели и основные задачи дисциплины достигаются

- проведением всех видов учебных занятий;
- осуществлением эффективного текущего и итогового контроля занятий и навыков студентов;
- организацией самостоятельной работы студентов.

Для достижения определенного квалификационной характеристикой уровня подготовки, в результате изучения дисциплины студенты должны

ЗНАТЬ

- основные факты, лежащие в основе построения теории информации и кодирование;
- основные положения и теоремы теории информации и кодирование.

УМЕТЬ

- применять методологические основы информации в практической деятельности;
- применять алгоритмы кодирования практической деятельности;
- применять алгоритмы сжатия данных в практической деятельности;
- применять цифровую подпись в практической деятельности;
- использовать криптографические методы в решении важных прикладных задач;
- ориентироваться в имеющейся литературе по теории информации и кодировании;
- самостоятельно расширять круг математических знаний по теории информации и кодировании, используя необходимую научную, учебную и справочную литературу.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

№ п/п	Наименование разделов, тем	Количество часов				
		Аудиторные				Самост. работа
		Лекции	Практ., семинары	Лаб. занятия	КСР	
1.	**Раздел I. Введение в курс. Основные понятия и определения**	**4**	**4**			
1.1.	Информация и виды информации.	2	2			
1.2.	Информация и энтропия.	2	2			
2.	**Раздел II.Теория информации и оптимальная кодировка.**	**12**	**12**	**4**		
2.1.	Системы исчисления. Общая характеристика кодов.	2	2			
2.2.	Введение в курс кодировки информации.	2	2			
2.3.	Алгоритмы кодировки информации.	2	2			
2.4.	Алгоритмы кодировки и сжатия информации.	2	2			
2.5.	Алгоритмы сжатия информации.	2	2	2		
2.6.	Алгоритмы адаптивного сжатия информации.	2	2	2		
3.	**Раздел III. Элементы криптологии.**	**12**	**12**	**8**		
3.1.	Введение в криптологию.	2	2			
3.2.	Введение в курс криптографических систем с секретными ключами.	2	2			
3.3.	Криптографические системы с секретными ключами.	2	2	2		
3.4.	Введение в курс криптографических систем с открытыми ключами.	2	2	2		
3.5.	Криптографические системы с открытыми ключами.	2	2	2		
3.6.	Криптографические системы с открытыми ключами и их анализ.	2	2	2		

Учебно-методическая карта

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов				Материальное обеспечение занятия (наглядные, методические пособия и др.)	Литература	Формы контроля знаний
		Лекции	Практические (семинарские) занятия	Лабораторные занятия	Контролируемая самостоятельная работа студента			
1	**2**					**7**	**8**	
1.	**Раздел I. Введение. Основные понятия и определения.**	**4**	**4**					
1.1..	**Информация, виды информации.** 1. Хранение, измерение, обработка и передача информации. 2. Способы измерения информации. **3.** Математические модели сигналов.	2	2				[1, 2, 3, 4, 5, 6]	
1.2.	**Информация и энтропия.** 1. Вероятностный подход к измерению дискретной и непрерывной информации. Смысл энтропии Шеннона. 2. Дифференциальная и относительная энтропия, максимум энтропии. 3. Энтропия дискретных случайных процессов. **4.** Эргодические и Марковские процессы.	2	2				[1, 2, 3, 4, 5, 6]	
2.	**Раздел II. Теория информации и оптимальная кодировка.**	**12**	**12**	**4**				
2.1.	**Системы исчисления. Общая характеристика кодов.** 1. Десятичная, двоичная, восьмеричная и шестнадцатиричная системы исчисления. 2. Код, кодировка. Одноэлементная и многоэлементная кодировки. Классификация кодов. **3.** Избыточная кодировка. Метрика Хемминга. Прин-	2	2				[1, 2, 3, 4, 5, 6]	

	ципы выявления и исправления ошибок избыточными кодами. **4.** Принцип максимальной правдоподобности.							
2.2.	**Введение в курс кодировки информации.** 1. Эффективное и оптимальное кодирование дискретного источника сообщений. 2. Теорема кодирования Шеннона. **3.** Побуквенное кодирование.	2	2				[1, 2, 4, 5, 11, 12]	
2.3.	**Алгоритмы кодировки информации.** 1. Сжатие данных и избыточность. **2.** Алгоритмы кодирования, применяемые в архиваторах. **3.** Интервальное кодирование и метод «стопка книг» **4.** LZ-кодирование информации.	2	2				[1, 2, 4, 5, 11, 12]	
2.4.	**Алгоритмы кодировки и сжатия информации.** 1. Сжатие информации с потерями. **2.** Сжатие информации с использованием преобразования Барроуза–Уилера.	2	2				[1, 2, 4, 5, 11, 12]	
2.5.	**Алгоритмы сжатия информации.** 1. Арифметическое кодирование. 2. Адаптивные алгоритмы сжатия. **3.** Кодирование Хаффмена.	2	2	2			[1, 2, 4, 5, 11, 12, 15, 16]	
2.6.	**Алгоритмы адаптивного сжатия информации.** 1. Адаптивное алгоритмическое сжатие. **2.** Методы Лемпела-Зива.	2	2	2			[1, 2, 4, 5, 11, 12, 15, 16]	
3.	**Раздел III. Элементы криптологии.**	**12**	**12**	**8**				
3.1.	**Введение в криптологию.** 1. Секретность и имитостойкость. 2. Основные идеи криптологии. **3.** Криптография и криптоанализ.	2	2				[1, 2, 5, 6, 10, 17]	
3.2.	**Введение в курс криптографических систем с секретными ключами.** 1. Введение в курс криптографических систем с секретными ключами. Подстановки и перестановки. 2. Полиалфавитные шифры.	2	2				[1, 2, 5, 6, 10, 17]	

	3. Шифр с бегущим ключом.							
3.3.	**Криптографические системы с секретными ключами.** 1. Теорема Шеннона о совершенно секретных шифрах. **2.** Криптосистемма DES (стандарт шифрования данных). **3.** Криптосистема ГОСТ.	2	2	2			[1, 2, 5, 6, 10, 17]	
3.4.	**Введение в курс криптографических систем с открытыми ключами.** 1. Введение в курс криптографических систем с открытыми ключами. **2.** Односторонняя функция с лазейкой. “Шарады” Меркля. **3.** Криптосистема Диффи и Хэллмана и проблема вычисления дискретного логарифма.	2	2	2			[1, 2, 5, 6, 10, 17, 18]	
3.5.	**Криптографические системы с открытыми ключами.** 1. Криптосистема RSA и проблема разложения числа на простые сомножители. 2. Криптосистема Меркля-Хэллмана, основанная на задаче об укладке ранца. **3.** Криптоанализ системы Меркля-Хэллмана.	2	2	2			[1, 2, 5, 6, 10, 17, 18]	
3.6.	**Криптографические системы с открытыми ключами и их анализ.** 1. Кодирующая система Мак Элиса. 2. Криптосистема Нидеррайтера. **3.** Цифровая подпись.	2	2	2			[1, 2, 5, 6, 10, 17, 18]	

ИНФОРМАЦИОННАЯ ЧАСТЬ

ЛИТЕРАТУРА

Основная

1. Кудряшов Б.Д. Теория информации: Учебник для вузов. – СПб.: Питер, 2009.
2. Колмогоров А.Н. Теория информации и теория алгоритмов. – М.: Наука, 1987.
3. Лидовский В.В. Теория информации: Учеб.пособие. – М.: Компания Спутник+, 2004.
4. Потапов В.Н. Введение в теорию информации: Учеб.пособие. – Новосибирск: Новосиб. гос. ун-т., 2009.
5. Самсонов Б.Б., Плохов Е.М., Филоненков А.И., Кречет Т.В. Теория информации и кодирование: Учеб.пособие. – Ростов-н/Д: Феникс, 2002.
6. Кузьмин И.В., Кедрус В.А. Основы теории информации и кодирования. – К.: Вища школа, 1986.
7. Хохлов Г.И. Основы теории информации: Учеб.пособие. – М.: Академия, 2008.
8. Шеннон К. Работы по теории информатики и кибернетики. М., 1963.
9. Нечаев В.И. элементы криптографии. Основы теории защиты информации. – М.: Высшая школа. 1999.

Дополнительная

10. Тарасенко Ф.П. Введение в курс теории информации / Ф.П. Тарасенко ¾ Томск: Изд-во Томского университета, 1963. ¾ 240 с.
11. Берлекэмп. Алгебраическая теория кодирования. Пер. с англ. – М.: Мир. 1971. – 477 с.
12. Блейхут Р. Теория и практика кодов, контролирующих ошибки. Пер. с англ. – М.: Мир. 1986. – 576 с.
13. Введение в криптографию. Под ред. В.В. Ященко. Москва, МЦНМО – ЧеРо, 1999.
14. Дориченко С.А. , Ященко В.В. 25 этюдов о шифрах. Москва, ТЕИС, 1994. 69 с.
15. КонвейДж.Н., СлоэнН.Дж.А. Упаковки шаров, решетки и группы. Пер. с англ. – М.: Мир. 1990. –I, II т.
16. Кричевский Р.Е. Сжатие и поиск информации. Наука, 1986.
17. Нечаев В.И. элементы криптографии. Основы теории защиты информации. – М.: Высшая школа. 1999. – 109 с.
18. Саломаа А. Криптография с открытым ключом. Пер. с англ. – М.: Мир. 1996. – 318 с.

ПРОТОКОЛ
СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ С ДРУГИМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Название дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы по изучаемой учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ
К УЧЕБНОЙ ПРОГРАММЕ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ
НА _2012____ / _2013_____ УЧЕБНЫЙ ГОД

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
_____ (протокол № ____ от _____ 200___ г.)
(название кафедры)

Заведующий кафедрой
_____
(степень, звание)(подпись)(И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета/Зав.общеуниверситетской кафедрой
_____ _____
(степень, звание)(подпись) (И.О.Фамилия)